REMARKS

Claims 13-30 are pending in the application. Claims 13-30 were rejected. Claims 13 and 17 are amended. Claims 19-24 are canceled. Claims 13-18 and 25-30 are now pending in the application. Claims 13 and 25 are the independent claims. Reconsideration of the amended application is respectfully requested.

The Examiner rejected claims 13-18 under 35 USC §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter that Applicants regard as the invention. In particular, the Examiner noted a lack of antecedent basis for a term in claim 13, which inadvertently was not amended in the previous response. Claim 13 is amended to correct the informality. Claim 17 is also amended to correct a typographical error. The rejection of claims 13-18, therefore, should be withdrawn.

The Examiner rejected claims 13-30 under 35 USC §103(a) as being unpatentable over Gullman et al., in view of Gennaro et al.

Independent claim 13 recites a method of authenticating the identity of a user to determine access to a system. According to the claimed method, a possession-based data instance, a modified version of the possession-based data instance, a knowledge-based data instance, a biometric-based data instance, and a modified version of the biometric-based data instance are provided. A first cryptographic key is generated based on the knowledge-based data instance, and is applied to the modified version of the possession-based data instance to generate a first recovered data instance. The first recovered data instance is interrogated against the possession-based data instance to generate a possession value as a result of a first correspondence evaluation. The first cryptographic

key is applied to the modified version of the biometric-based data instance to generate a second recovered data instance. The second recovered data instance is interrogated against the biometric-based data instance to generate a biometric value as a result of a second correspondence evaluation. The first cryptographic key, the possession value, and the biometric value are combined to form a second cryptographic key. The user's access to the system is restricted if the user's identity is not authenticated, based at least in part on the second cryptographic key; alternatively, the user's access to the system is granted if the user's identity is authenticated, based at least in part on the second cryptographic key.

In contrast, Gullman et al. disclose a system including a biometric security apparatus, an access device, and a host system. The biometric security apparatus and access device work together to authenticate users as a security safeguard for the host system by combining biometric data with other identifying and control data to issue a security token that the host system evaluates to determine if a user is authorized to access the host system. The biometric security apparatus can be embodied in a portable integrated circuit card. As in claim 13, Gullman et al. utilize possession-based data, in the form of a fixed code stored in ROM 24 on the biometric security apparatus. Gullman et al. can also utilize knowledge-based data, in the form of a challenge code provided by the host system that must be entered by the user as part of the authentication process. The biometric data, challenge code, and possession-based data are used to create the security token, which the host systems evaluates to determine authentication.

However, Gullman et al. do not provide a modified version of the possession-based data instance, which is decrypted to generate a first recovered data instance that is

interrogated against the possession-based data instance to generate a possession value that is used as a component of the security token. Rather, Gullman et al. use the fixed code directly as the possession value. Likewise, Gullman et al. do not provide a modified version of the biometric-based data instance, which is decrypted to generate a second recovered data instance that is interrogated against the biometric-based data instance to generate a biometric value that is used as a component of the security token. Rather, Gullman et al. use the biometric information directly as the biometric value. The constructed security token can be encrypted before presentation to the host system, but modified possession and biometric components are not provided, as required by claim 13.

Gennaro et al. disclose a biometric authentication system having encrypted models. According to Gennaro et al., a biometric model is created from a biometric sample, and an encryption key is created from a password input. The encryption key is used to encrypt the biometric model. During an authentication process, the user enters a knowledge-based data instance, that is, his or her password. This password is used to create a key that is used to decrypt the stored encrypted biometric model, which is correlated against a newly-provided biometric input. However, the password is never used to recover a possession-based data instance from a modified version of the possession-based data instance. A subset of challenge answers is encrypted and stored with the biometric model, but this is knowledge-based data, not possession-based data (Gennaro et al. do not disclose possession-based data). Gennaro et al. do not disclose a possession-based data instance that is encrypted or otherwise modified and recovered for interrogation against the possession-based data instance, nor did the Examiner specifically assert that either reference discloses this feature. This modification and

recovery of the possession-based data instance is important, for example, in safeguarding against corruption of the possession-based data, which by its nature is disposed on a portable substrate that is subject to physical abuse.

Because neither Gullman et al. nor Gennaro et al. disclose a possession-based data instance that is modified and recovered, using a key derived from a knowledge-based data instance, for interrogation against the possession-based data instance, no combination of the cited references can disclose this feature of the invention as recited in claim 13. Neither reference discloses or suggests this feature, nor does either reference disclose or suggest any advantage to providing this feature. Because the combination of the teachings of the cited references does not disclose this recited feature, no combination of the references can render obvious the claimed invention. The rejection of claim 13, therefore, should be withdrawn. Claims 14-18 depend from claim 13, and therefore also cannot be rendered obvious by any combination of the teachings of the cited references. The rejection of claims 14-18, therefore, should be withdrawn as well.

Claims 19-24 are canceled without prejudice or disclaimer to the recited subject matter.

Independent claim 25 recites a method of authenticating the identity of a user to determine access to a system. A possession-based data instance, a biometric-based data instance, and a modified version of the biometric-based data instance are provided. The possession-based data instance is applied to the modified version of the biometric-based data instance to generate a recovered data instance. The recovered data instance is interrogated against the biometric-based data instance to generate a biometric value as a result of a correspondence evaluation. The possession-based data instance and the

biometric value are combined to form a cryptographic key, which is evaluated to determine if the user's identity is authenticated. The user's access to the system is restricted if the user's identity is not authenticated, based at least in part on the cryptographic key; alternatively, the user's access to the system is granted if the user's identity is authenticated, based at least in part on the cryptographic key.

In contrast, Gullman et al. disclose a system including a biometric security apparatus, an access device, and a host system. The biometric security apparatus and access device work together to authenticate users as a security safeguard for the host system by combining biometric data with other identifying and control data to issue a security token that the host system evaluates to determine if a user is authorized to access the host system. The biometric security apparatus can be embodied in a portable integrated circuit card. As in claim 25, Gullman et al. utilize possession-based data, in the form of a fixed code stored in ROM 24 on the biometric security apparatus. The biometric data and possession-based data are used to create the security token, which the host systems evaluates to determine authentication.

However, Gullman et al. do not provide a modified version of the biometric-based data instance, which is recovered and interrogated against the biometric-based data instance to generate a biometric value that is used as a component of the security token. Rather, Gullman et al. use the biometric information directly as the biometric value. The constructed security token can be encrypted before presentation to the host system, but a modified biometric component is not provided, as required by claim 25.

Gennaro et al. disclose a biometric authentication system having encrypted models. According to Gennaro et al., a biometric model is created from a biometric

sample, and an encryption key is created from a password input. The encryption key is used to encrypt the biometric model. During an authentication process, the user enters a knowledge-based data instance, that is, his or her password. This password is used to create a key that is used to decrypt the stored encrypted biometric model, which is correlated against a newly-provided biometric input. However, the password is a knowledge-based data instance, not a possession-based data instance. A subset of challenge answers is encrypted and stored with the biometric model, but this also is knowledge-based data, and is not used to decrypt the encrypted biometric model. In fact, Gennaro et al. do not disclose any possession-based data used as part of the authentication process. Gennaro et al. do not disclose a possession-based data instance that is used to decrypt or otherwise recover a modified biometric-based data instance for interrogation against the biometric -based data instance, nor did the Examiner specifically assert that either reference discloses this feature. This modification and recovery based on the possession-based data instance is important, for example, in detecting corruption of the possession-based data, which by its nature is disposed on a portable substrate that is subject to physical abuse.

Because neither Gullman et al. nor Gennaro et al. disclose a possession-based data instance that is used to decrypt or otherwise recover a modified biometric-based data instance for interrogation against the biometric-based data instance, no combination of the cited references can disclose this feature of the invention as recited in claim 25. Neither reference discloses or suggests this feature, nor does either reference disclose or suggest any advantage to providing this feature. Because the combination of the teachings of the cited references does not disclose this recited feature, no combination of

the references can render obvious the claimed invention. The rejection of claim 25, therefore, should be withdrawn. Claims 26-30 depend from claim 25, and therefore also cannot be rendered obvious by any combination of the teachings of the cited references. The rejection of claims 26-30, therefore, should be withdrawn as well.

Based on the foregoing, it is submitted that all rejections have been overcome. It is therefore requested that the Amendment be entered, the claims allowed, and the case passed to issue.

Respectfully submitted,

June 7, 2004
Date

Thomas M. Champagne
Registration No. 36,478
IP STRATEGIES
12 ½ Wall Street
Suite I
Asheville, North Carolina 28801
828.253.8600
828.253.8620 fax

TMC:hlp